FINAL EVALUATION REPORT

LUCENT TECHNOLOGIES

LUCENT MANAGED FIREWALL VERSION 3.0

FINAL
MARCH 1999

PREPARED BY:
COMPUTER SCIENCES CORPORATION
7471 CANDLEWOOD ROAD
HANOVER, MD 21076

PREPARED FOR:
LUCENT TECHNOLOGIES
480 RED HILL ROAD
MIDDLETOWN, NY 07748

SUBMITTED TO:
TTAP OVERSIGHT BOARD
9800 SAVAGE RD
FT. MEADE, MD 20755

FOREWORD

This publication, the Lucent Managed Firewall Final Evaluation Report, is being issued by Computer Sciences Corporation. This report is the principle source of information used by the Trust Technology Assessment Program (TTAP) Oversight Board to render a certification rating for the Lucent Managed Firewall. It is intended to support the TTAP certification process by providing all the information needed by the TTAP Oversight Board to verify the results of the evaluation. This report presents all evaluation results, their justifications, and any findings derived from the work performed during the evaluation. The requirements stated in this report are taken from the *Lucent Managed Firewall 3.0 Security Target* and conform to the *Common Criteria for Information Technology Security Evaluation*, Version 2.0.

ACKNOWLEDGMENTS

Evaluation Team Members

Computer Sciences Corporation

Reid Reininger

Cornelius Haley

Douglas Stuart

Vince Ritts, CISSP

Patrick Dunn, CISSP

MitreTek

Rick Murphy

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This document describes the results of Trust Technology Assessment Program (TTAP) evaluation of the security protection provided by the Lucent Managed Firewall (LMF) Version 3.0 configured as described in the [LMF_IGS] document. The security features of the LMF were examined against the requirements specified in the [LMF_ST] in order to establish a candidate rating.

The version of the product evaluated was LMF Version 3.0 (build 150). This product is also described in this report as the Target of Evaluation (TOE). The developer for the product was Lucent Technologies.

The purpose of the Lucent Managed Firewall is to provide controlled and audited access to specific Internet Protocol (IP) services, both from inside and outside an organization's network, by allowing, denying, and/or redirecting the flow of data through the firewall. The Lucent Managed Firewall selectively routes information flows among internal and external networks according to a site's security policy rules. By default, these security policy rules deny all inbound information flows. Only an authorized administrator has the authority to change the security policy rules. The Lucent Managed Firewall has the ability to make filtering decisions based on the source IP address, destination IP address, transport layer protocol, source port, destination port, and on the interface on which the packet arrives or goes out.

A Lucent Managed Firewall System Administrator configures the networking parameters of the firewall and creates Zone Administrator accounts. One or more Zone Administrators implement the site's security policies by defining a set of rules within their security zone. Each security zone is then applied to a physical network interface or to a contiguous range of IP addresses processed by the physical network interface. In this manner, a single Lucent Managed Firewall can enforce multiple, separately managed security policies.

The Lucent Managed Firewall provides controlled and centralized auditing functionality through a management server. All audit records are stamped with a dependable date and time. Auditable events include, but are not limited to, modifications to the group of users associated with the authorized administrator role, all use of the identification and authentication mechanisms, and all information flow control decisions made by the Lucent Managed Firewall according to the security policy rules. The Lucent Managed Firewall includes a reporting tool that allows searching and sorting of the collected audit trail data.

The Lucent Managed Firewall architecture consists of two physically distinct components: the firewall appliance, which controls the flow of traffic between network interfaces; and the Security Management Server, which allows the System Administrators and Zone Administrators to manage the firewall appliance.

The firewall function is physically separated from its management server, with the firewall code running on Inferno(tm), a Bell Labs-developed operating system. The Lucent Managed Firewall Security Management Server runs on both the Windows NT(tm) and Solaris platforms. However, only the version running on the Windows NT platform has been evaluated.

It is assumed the TOE is located within a controlled access facility that mitigates unauthorized physical access and the TOE is only used for firewall functionality. The TOE administrator is the only person allowed access to the TOE; there are no non-administrative accounts on the TOE. The administrator is assumed to be trustworthy and trained on security policies and practices of the environment for which the TOE is intended to protect. The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of the information in both the internal and external networks is equivalent.

The evaluation was carried out in accordance to the TTAP process and scheme described in *Proposed TTAP Process for Common Criteria EAL 1&2 Evaluations* and *TTAP Scheme*. The purpose of the evaluation was to demonstrate that the TOE meets the security requirements contained in the [LMF_ST]. The criteria against which the TOE was judged are described in the *Common Criteria for Information Technology Security Evaluation*. Two certifiers on behalf of the TTAP Oversight Board monitored the evaluation carried out by Computer Sciences Corporation. The evaluation was completed in December 1998.

Computer Sciences Corporation has determined that the [LMF_ST] was a valid target for evaluation, and it was used as the basis for the TOE evaluation of the LMF. Computer Sciences Corporation has determined that the evaluation assurance level (EAL) for the product, as specified in the [LMF_ST], is EAL2 and the product satisfies all the security functional requirements stated in the [LMF_ST].

1 Introduction

This document describes the results of Trust Technology Assessment Program (TTAP) evaluation of the security protection provided by the Lucent Managed Firewall (LMF) Version 3.0 and configured as described in the [LMF_IGS] document. The security features of the LMF were examined against the requirements specified in the [LMF_ST] in order to establish a candidate rating.

The evaluation was carried out in accordance to the TTAP process and scheme described in *Proposed TTAP Process for Common Criteria EAL 1&2 Evaluations* and *TTAP Scheme*. The purpose of the evaluation was to demonstrate that the TOE meets the security requirements contained in the [LMF_ST]. The criteria against which the TOE was judged are described in the *Common Criteria for Information Technology Security Evaluation*. The evaluation was completed in December 1998.

Computer Sciences Corporation has determined that the [LMF_ST] was a valid target for evaluation, and it was used as the basis for the TOE evaluation of the LMF. Computer Sciences Corporation has determined that the evaluation assurance level (EAL) for the product, as specified in the [LMF_ST], is EAL2 and the product satisfies all the security functional requirements stated in the [LMF_ST].

1.1 Background

The TTAP is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called TTAP Evaluation Facilities (TEFs) using the current NSA evaluation methodology and proposed evaluation methodology for Evaluation Assurance Level (EAL)1 and EAL2 in accordance with cooperative research and development agreements. The program focuses on products with features and assurances characterized by the Trusted Computer System Evaluation Criteria (TCSEC) C2 and B1 level of trust and the Common Criteria (CC) EAL1 through EAL4.

The TTAP Oversight Board monitors the TEFs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a TEF and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is to be added to NSA's Evaluated Products List.

1.2 Document Organization

This document consists of ten chapters and one supporting appendix. Chapter 1 provides an introduction and overview of the evaluation process. Chapter 2 identifies the TOE and describes the evaluated configuration. Chapter 3 describes the security policy that the TOE has been designed to enforce. Chapter 4 describes the assumptions and clarifies the scope of the evaluation. Chapter 5 identifies the documents that were provided as evaluation deliverables. Chapter 6 describes the functional testing performed by the developer and the evaluation team to ensure that the product satisfies the stated security functional requirements. Chapter 7 provides a description of the results of the evaluation. Chapter 8 provides the conclusions and recommendations of the evaluation team. Chapter 9 provides a glossary of acronyms that are used throughout the evaluation documentation. Chapter 10 provides the bibliography of documents that were used throughout the evaluation process. Annex A provides the [LMF_ST].

2 Identification

Table 1 identifies the hardware and software components that compose the evaluated version of the LMF.

Table 1: TOE Identification

TOE Device	Components	
	Hardware	**Software**
Firewall Appliance	Model 201 ➢ Four Intel 10/100Base-T Ethernet interface cards ➢ Pentium II 333MHz processor ➢ Tyan Tsunami ATX Version 1.07 motherboard ➢ 64MBytes of RAM	➢ Inferno (LMF internal release version only)
Security Management Server	➢ 200MHz Pentium-pro processor (or better) ➢ 96MBytes system memory ➢ 2GB Hard Drive (minimum) ➢ CD-ROM Drive ➢ Ethernet interface card ➢ Video card- must be capable of 1024x768 resolution with 65,535 colors ➢ Backup device	➢ Microsoft Windows NT 4.0 ➢ Microsoft Windows NT 4.0 Service Pack 3 ➢ Netscape Communicator 4.05 ➢ Netscape Enterprise Server 3.5.1 (with Java enabled) ➢ LMF version 3.0 (Build 150)

2.1 Evaluated configuration

2.1.1 Network architecture

The FA device has four network interfaces and is the central network device in this system. The configuration used by the evaluation team ensured that the firewall was tested without having to rely on other network devices to provide supporting security functionality. This enabled testing and analysis of the LMF as a separate entity placing assurance on the LMF components rather than supporting network devices. Therefore, if the System Administrator follows the guidance provided in the [LMF_IGS] and [LMF_AGD] documents and installs the product in the evaluated configuration, the LMF is able to be installed in conjunction with any other supporting network devices.

The network architecture illustrated in Figure 1 identifies the FA device and its four network interfaces as well as the supporting SMS. The evaluated configuration must have the SMS connected to one of the FA's network interfaces in a logically and physically isolated protected network. In addition, the network architecture must have the concept of at least one protected network and an external network. The FA device has four network interfaces, and another protected network can be associated with the fourth network interface (such as a DMZ). Note, however, that a configuration that consists of one protected domain and two untrusted domains falls outside the evaluated configuration.

The evaluated configuration only allows having the management server installed on a Windows NT workstation. In addition, to meet the security functional requirements, the evaluated configuration allows only a single FA being managed by a single SMS. This ensures that the order of occurrence is maintained within the audit files.

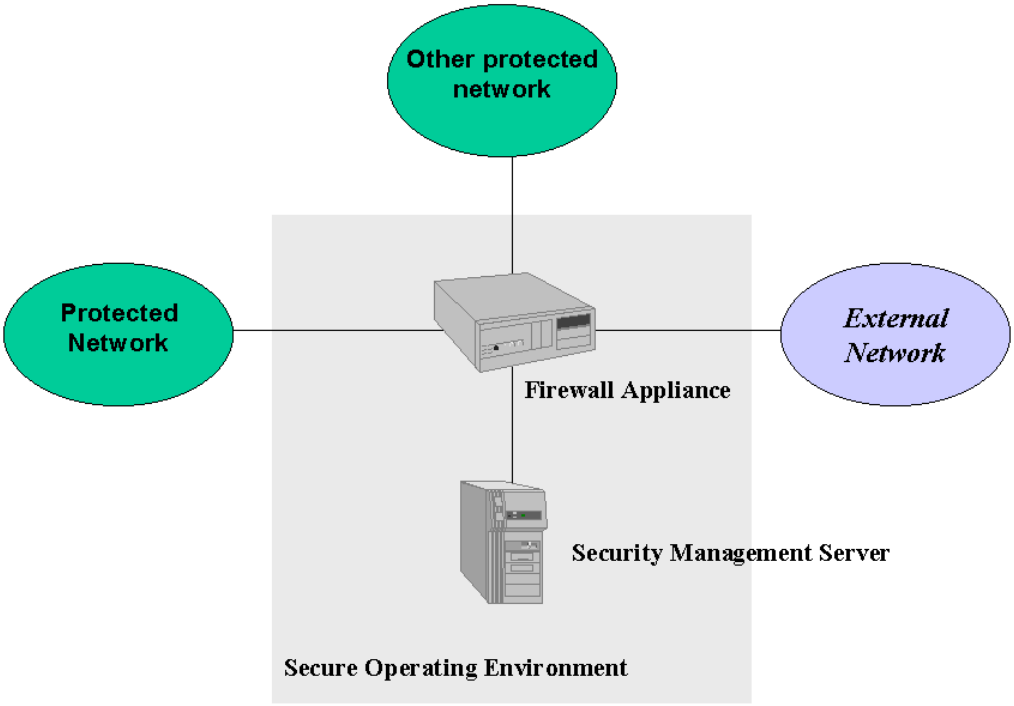

Figure 1: Evaluated network configuration

2.1.2 Required Configuration Parameters

2.1.2.1 SMS Configuration

The SMS provides management functions for the LMF and therefore many of the configuration settings can be made through the management server. There are several configuration settings, which must be made by the System Administrator to ensure that the SFRs described in the [LMF_ST] are met. These configuration details are provided in the [LMF_IGS] and can be summarized as follows:

a) The SMS host operating system must audit the shutdown of the SMS application.

b) The SMS host operating system must audit use of the identification and authentication mechanisms of the SMS host operating system.

c) The SMS host operating system must audit changes to user accounts on the SMS host.

d) The SMS host operating system must audit any access to the audit files.

e) The SMS host operating system must audit changes to the time on the SMS host.

f) The directory and file permissions of the SMS host must be set to protect the audit records.

g) The directory and file permissions of the SMS host must be set to protect the SMS software.

h) A unique administrator account must be supplied on the SMS host operating system for each identified SMS System Administrator.

i) The FA must be configured to stop processing when communications have been lost with the SMS.

2.1.2.2 FA Configuration

The initial configuration of the FA device is performed by creating a configuration floppy disk with the SMS and then booting the FA device from the floppy disk. The initial configuration will provide the FA with its own address and that of the SMS and the other two network interfaces. This allows the FA device to establish a communications path with its management server. The SMS provides the interface for the System Administrator to configure several parameters, which affect the operation of the LMF. These parameters are configured by the System Administrator through the SMS GUI interface and can be downloaded to the FA device via the established communications path.

2.1.2.3 Network Addressing Requirements

The FA device has the ability to operate at the data-link layer as a bridge device. This state of operation does not allow the LMF to meet several of the requirements identified in the [LMF_ST]. However, the FA device can be configured to operate at the network layer and have IP addresses associated with each of the network interfaces. The evaluated configuration requires that each network interface be configured to have an IP address rather than appearing invisible at the network layer. In addition, it is important that each of the FA device's network interfaces is configured to be on a separate subnet. This configuration is required to meet the requirements stated in the [LMF_ST].[1]

2.1.2.4 Mandatory Rule Set

In order for the LMF to meet the requirements of the FDP_IFF.1 – Simple Security Attributes, there are several rules that must be enforced. These policy rules must be enforced on each of the security zones that are assigned to the internal or external network interfaces.

[1] For a detailed description of why the evaluators have mandated this configuration, see commentary provided Section 7.2.14 of this report.

The FA device has four external Ethernet interfaces and each of these must be assigned a security zone that reflects the requirements set by FDP_IFF.1. The interface that has the SMS connected will automatically have an assigned zone to protect the SMS. This security zone should not be altered. However, the rules sets identified in Table 2 must be applied to each of the other three interfaces.

Table 2: Mandatory rules for all zones

Direction	Source	Destination	Port	Action
⇔Z	Loopback	*	*	Drop
⇔Z	*	Loopback	*	Drop
⇔Z	Broadcast	*	*	Drop
⇔Z	*	Broadcast	*	Drop
⇔Z	Firewall-Address	*	*	Drop
⇔Z	*	Firewall-Address	*	Drop

The rule sets defined in Table 2 identify the restriction on loopback and broadcast addresses as source addresses. In addition, a rule is defined to protect the FA from external packets claiming to be from the FA address. Table 3 also provides a listing of the required Host Groups to define the rule sets of Table 2.

Table 3: Host Groups

Host Group	Description
Broadcast	A group that defines the set of broadcast host addresses that the FA device is capable of determining.[2]
Loopback	The set of loopback addresses – 127.*.*.*
Internal-Zone-Addresses	A group that defines the range of valid addresses on the internal (protected) network.
Zone-Addresses	A set of internal address ranges that apply to a single zone.
Firewall-Addresses	The set of addresses that relate to the FA device's network interfaces.

2.1.2.5 Internal Zone Rule Set

A rule set must be applied to each of the network interfaces that have been identified as being an internal or protected network. Table 4 identifies the rule set that must be applied to the internal networks by the System Administrator to ensure that the requirements of the [LMF_ST] have been met. It is important that the order of the rules in the zone table is maintained as the LMF enforces the rules in the order that they appear in the table. A description for each of the rules is provided as follows:

a) ***Rule 1***. This indicates that the mandatory rules defined in Table 2 must appear first in the zone rule table.

b) ***Rule 2***. A packet leaving the internal zone must not have a destination address that translates to an address of that zone.

c) ***Rule 3***. A packet entering the internal zone must not have a source address that translates to an address associated with that zone.

[2] A broadcast address is defined as a host address comprising all ones or all zeros, and complete IP address comprising all ones. For further information see RFC1700.

d) ***Rule 4***. This rule provides guidance to the System Administrator for developing a pass rule for the packets that are entering the zone. If the System Administrator creates a rule to allow a packet to enter the zone, then the packet's destination address must be in that zone's host group.

e) ***Rule 5***. This rule provides guidance to the System Administrator for developing a pass rule for packets that are leaving the zone. If the System Administrator creates a rule to allow packets to leave a zone, then the source address of the packet must have a source address that is present in the zone's host group.

f) ***Rule 6***. This is the last rule in the table and ensures that any information flow that has not been explicitly allowed will be denied. By default, this is the only rule present when a new zone is created.

Table 4: Internal Zone Rule Set

Rule No.	Direction	Source	Destination	Port	Action
1	*Mandatory rule set from Table 2*				
2	⇐Z	*	Zone-Address(i)	*	Drop
3	⇒Z	Zone-Address(i)	*	*	Drop
4	⇒Z	?	Zone-Address(i)	?	Pass
5	⇐Z	Zone-Address(i)	?	?	Pass
6	⇔Z	*	*	*	Drop

2.1.2.6 External Zone Rule Set

A rule set must also be defined for the designated external network interface. Table 5 identifies the rule set that must be defined by the System Administrator to ensure that the requirements of the [LMF_ST] have been met. It is important that the order of the rules in the zone table is maintained as the LMF enforces the rules in the order that they appear in the table. A description for each of the rules is provided as follows:

a) ***Rule 1***. This indicates that the mandatory rules identified in Table 2 must appear first in the zone rule table.

b) ***Rule 2***. This rule must be repeated for all zones that have been defined in the policy as internal. A packet leaving the external zone and entering an internal zone must not have a source address that translates to a defined internal host group(s).

c) ***Rule 3***. This rule must be repeated for all zones that have been defined in the policy as internal. A packet entering the external zone from an internal zone must not have a destination address that translates to an address defined in an internal host group(s).

d) ***Rule 4***. This rule provides guidance to the System Administrator for developing pass rules for packets leaving the external zone and entering an internal zone. If the System Administrator wishes to create a rule to allow a packet to leave the zone, then the destination address must appear in one of the host groups defined for an internal protected network(s).

e) ***Rule 5***. This rule provides guidance to the System Administrator for developing pass rules for packets entering the zone. If the System Administrator wishes to create a rule to allow a packet to enter to the external zone form an internal zone, then the source address must be contained in one of the defined host groups on an internal network(s).

f) ***Rule 6***. This is the last rule in the table and ensures that any information flow that has not been explicitly allowed will be denied. By default, this is the only rule present when a new zone is created.

Table 5: External Zone Rule Set

Rule No.	Direction	Source	Destination	Port	Action
1	*Mandatory rule set from Table 2*				
2	⇐Z	Internal-Zone-Address(0….n)	*	*	Drop
3	⇒Z	*	Internal-Zone-Address(0….n)	*	Drop
4	⇐Z	?	Internal-Zone-Address(0….n)	?	Pass
5	⇒Z	Internal-Zone-Address(0….n)	?	?	Pass
6	⇔Z	*	*	*	Drop

2.1.3 Other Considerations

The administration of the LMF utilizes a Netscape browser (the actual GUI), a set of SMS services (for interpreting communication from the GUI and FA), and the FA (which performs actual traffic filtering). In the COTS LMF product, communication between the Netscape browser is encrypted by an SSL encrypted session. The communication between SMS services and the FA utilize an encrypted IP session.

Since neither the SSL or IP session encryption are included as part of the evaluation, no protection can be assumed for these communication paths. Therefore, physical isolation and protection measures must be utilized to provide the necessary privacy of communications in an evaluated configuration. In fact, in the evaluated configuration, not only must the SMS and the FA be isolated and protected but also the Netscape browser must be executed only from the SMS. The [LMF_IGS] and the [LMF_ST] provides a description of this configuration.

2.2 System overview

The Lucent Managed Firewall architecture consists of two physically distinct components:

a) The FA, which controls the flow of traffic between network interfaces.

b) The SMS, which allows the System Administrator to manage the security the Firewall Appliance.

The firewall function is physically separated from its management server, with the firewall code running on Inferno™, a Bell Labs-developed operating system. The Security Management Server software of the evaluated TOE runs on the Windows NT™ platforms.

2.3 Hardware Overview

For an EAL2 evaluation, the design documentation is not required to provide a detailed description of the supporting hardware of the TOE if it does not provide a security enforcing function. Therefore, to ensure that the TOE's hardware and associated mechanisms support self-protection and non-bypassability, the evaluation team placed emphasis on these aspects during the functional and penetration testing of the product. All testing performed indicated that the LMF hardware and the associated mechanisms supported the security functionality of the TOE.

2.3.1 SMS Hardware

The evaluated configuration requires that the SMS software be installed on a dedicated host that is connected to the FA device through a direct network connection. The SMS host should not have any processes or software installed that do not support the security functionality of the LMF. The SMS's isolation from user networks provides a secure operating domain for the SMS software. In addition, the communications between the FA device and the SMS host are authenticated and encrypted ensuring that only the FA device is able to communicate with the SMS host.

The SMS software of the evaluated TOE runs on the Windows NT 4.0 operating system. The hardware for the SMS workstation used during the testing phases of the evaluation had the following specifications:

a) Pentium II 333MHz processor (or better)

b) 96MB system memory

c) 2GB hard drive

d) CD-ROM drive

e) One 10/100Base-T Ethernet network card

f) Video card 1024 x 768 resolution with 65,535 colors

g) Backup device

2.3.2 FA Hardware

The FA hardware provides a secure domain for the firewall software to operate in. The memory management techniques and supporting hardware of the FA device ensure that the TSP of the TOE executes in a domain of its own. Information and processes received from external IT entities are unable to execute processes in that domain. Processes executed in response to the receipt of information from external IT entities are handled as separate processes and they cannot interfere with other processes being managed by the TOE. These arguments were supported by both functional and vulnerability testing performed by the evaluation team

The evaluated FA is the Model 201. This device has the following hardware specifications:

a) 19” rack mountable case

b) 120 Volt AC power supply

c) Four Intel 10/100Base-T Ethernet interface cards

d) Pentium II 333MHz processor

e) Tyan Tsunami ATX Version 1.07 motherboard

f) 64MBytes of RAM

The evaluated version of the FA is equipped with four 10/100Base-T Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs).

The Firewall Appliance is not shipped with a monitor, keyboard, or hard disk. Other than a floppy disk drive for initial software boot, it has minimal moving parts (an on/off switch and a power supply fan). The brick initially boots from a floppy diskette that is created by the SMS.

2.4 Software overview

2.4.1 FA Software

The firewall software that runs on the FA is based on the Inferno™ operating system, a small Bell Labs-developed operating system. The firewall code is embedded within the Inferno™ operating system kernel.

The FA communicates with the SMS using IP. Accordingly, the FA must be assigned a logical IP address. The FA must be configured to communicate only with the SMS’s network address, dropping all other communication attempts, and thus remaining invisible to all other network addresses.

All communications between a FA and the SMS are encrypted and authenticated using proprietary Inferno™ encryption and authentication mechanisms (Diffie Hellman for key exchange, ElGamal for digital signatures and signature verification, and DES for session encryption).[3]

The packets that are received from the internal and external networks are not able to execute or perform any processes on the FA device. The FA software ensures that packets are received from the internal or external network and are then either passed through or dropped. Processes executed in response to the receipt of information from external IT entities are handled as separate processes and they cannot interfere with other processes being managed by the TOE.

2.4.1.1 Decision Module

The FA will perform decision making on information contained within an IP datagram. The decision module extracts information from the IP datagram and applies a set of rules, derived from the security policy, to the information to determine whether to pass or drop the datagram. The decision module enforces the security policy derived from the set of security zone policies that have been assigned to the network interfaces of the FA device.

Information within an IP packet that is used to make access control decisions includes source IP address, destination IP address, transport layer protocol, source port, destination port. In addition, time-of-day, day-of-week, direction of access, physical Ethernet port, and existing session information can be used to determine whether or not a packet is allowed to pass. If the decision is to permit the packet to pass, the decision module determines which Ethernet port(s) will receive the datagram.

The Decision Module operates within the secure domain of the firewall application running on the Inferno software. The Decision Module does not process packets from the internal or external networks. The firewall application receives the packets and places them in a buffer, at which point the Decision Module is then required to make a decision on whether the firewall application should pass or drop the packet. Therefore, the Decision Module is protected from tampering.

2.4.1.2 Session Cache Module

The session cache module retains the access control decision result for use with future packets from the same session. When a packet that is part of an established session arrives at the firewall, the decision module can first check the session cache to determine if the packet is authorized.

The Session Cache module does not interact with external information. This module only has the function of monitoring the establishment of sessions between external IT entities that the FA device is filtering.

[3] This evaluation did not include analysis of the encryption mechanisms of the LMF. The evaluation team is unable to provide any assurance for the secure operation of these mechanisms.

2.4.1.3 Audit Module

The audit module records the start and end of a session. It extracts information from the session cache to uniquely identify each session and produce an audit record for each successful and unsuccessful session for the FA device. The audit module bundles this information into an audit message and sends it to an awaiting audit server, located on the SMS.

The audit module is also protected and cannot be tampered by external processes. The audit module receives information from the Session Cache Module and the Decision Module and passes this information to the Administration Application. There are no external interfaces available to the Audit Module.

2.4.1.4 Administration Applications

The administration applications permit the security policies to be remotely loaded in the FA device from the SMS over an authenticated and encrypted session. Each security policy's digital signature is verified before the policy is loaded. (The policies are digitally signed by the Security Management Server using the firewall administrator's certificate when created or edited.) The administration applications also provide system status information to the SMS.

The Administration Application is configured to communicate directly with the SMS. This communication is encrypted and authenticated, and only the Application Module will service requests form the SMS. The evaluated configuration ensures that the Administration Application is only communicating with the SMS on the configured network interface.

2.4.2 SMS Software

The SMS software provides the tools to manage the security policies of the security zones that are applied to the FA device. The software runs at the application layer using hosted Inferno™ and Java™ on Windows NT™. The SMS implements and enforces an administrator privilege model. Two categories of administrators can be created: system administrators and security zone administrators. System administrators control the entire system infrastructure (such as which security zones are applied to which bricks), whereas security zone administrators control only their specific security zone. The privilege to create additional administrator accounts can be assigned to specific administrators.

Within a security zone account, the security zone administrator can be assigned create, create/edit, or create/edit/load privileges for managing the security policy within that security zone. The privilege model is maintained entirely within the Security Management Server and is not reliant upon OS-level user accounts or authentication. The primary components of the SMS software are hosted Inferno daemons, Java™ server-side applications, and a graphical user interface.

3 Security Policy

3.1 Policy Overview

The LMF is intended to enforce a system security policy, through several zone security policies, which controls the flow of information through the firewall. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities. The information flowing between subjects is defined as traffic with attributes.

The LMF has been designed to enforce the information flow control security policy on unauthenticated external IT entities that either send or receive information through the TOE. An external IT entity is identified by an IP address. The information or traffic is defined as an IP datagram. Therefore, information attempting to pass through the TOE that does not have the attributes of an IP datagram shall be denied.

To meet the requirements of the information flow security policy defined in the [LMF_ST], a rule set has been defined in the [LMF_IGS] document. This rule set must be applied to the FA device to enforce the information flow security policy. This rule set is defined in Section 2.1 of this document.

3.2 Policy Security Attributes

The LMF must make a decision to either pass or drop traffic according to the values of the security attributes contained within the traffic. This decision is made according to a specific information flow control policy defined by the System Administrator to meet the needs of the organization.

The System Administrator is able to implement the specific organization security policy by defining a rule set with the following information security attributes:

a) presumed IP address of source subject

b) presumed IP address of destination subject

c) transport layer protocol

d) TOE interface on which traffic arrives and departs

e) service

3.3 Information Flow Security Policy

The LMF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

   i) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.

   ii) The presumed address of the source subject, in the information, translates to an internal network address.

   iii) The presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

   i) All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator.

   ii) The presumed address of the source subject, in the information, translates to an external network address.

   iii) The presumed address of the destination subject, in the information, translates to an address on the other connected network.

The LMF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network.

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.

4 Assumptions and clarification of scope

The TOE is intended to be used in environments in which either, at most, sensitive but unclassified information is processed, or the sensitivity level of the information in both the internal and external networks is equivalent.

4.1 Usage assumptions

The assumptions made about the usage of the TOE are identified in Section 3.1, Assumptions, of the *Lucent Managed Firewall Version 3.0 Security Target.*

4.2 Environmental assumptions

The assumptions about the environment for which the TOE is to be used are identified in Section 3.1, Assumptions, of the *Lucent Managed Firewall Version 3.0 Security Target.*

4.3 Clarification of scope

The threats addressed by the TOE and for which specific protection within the TOE or its environment is required are described in Section 3.2, Threats, in the *Lucent Managed Firewall Version 3.0 Security Target.* The IT security requirements of the TOE are traceable to security objectives derived from the assumptions and threats identified in Section 3.0, TOE Security Environment, of the *Lucent Managed Firewall Version 3.0 Security Target.* Threats that are not listed in Section 3.2 are not recognized as being addressed by the TOE because the IT security requirements for which the TOE was evaluated were not derived to counter these threats. Thus, no assumptions or claims can be made about the ability of the TOE to counter threats not specified in Section 3.2.

5 Documentation

Table 6 provides a listing of the LMF documents that are to be provided to the customer.

Table 6: Evaluation Deliverables

Identifier	Date	Version	Name
LMF_ST	12/22/98	1.3	Lucent Managed Firewall Security Target
LMF_SAR	Nov. 98	3.0	Lucent Managed Firewall System Administrator Reference Manual
LMF_BIG	Nov. 98	3.0	Lucent Managed Firewall Brick Installation Guide
LMF_IG	Nov. 98	3.0	Lucent Managed Firewall Installation Guide
LMF_IGS	Nov. 98	8.0	Lucent Managed Firewall Installation, Generation and Start-up
LMF_AGD	Dec. 98	1.0	Lucent Managed Firewall Administrator Guidance

6 Product testing

6.1 Testing Coverage

Lucent testing documentation consists primarily of Excel Spreadsheets, which enumerate the test cases performed by testers and record the result of each test case. Review of these spreadsheets by the evaluation team showed that the following set of spreadsheets completely covers the TOE security functions that satisfy the security functional requirements from the Security Target.

a) LMF 3.0 Release Test Cases

b) Test Cases for Download (Release 3.0)

c) LMF 3.0, non-IP Protocol Feature Test cases

d) Les Midouin - Test cases for Release 3.0

e) Lucent Managed Firewall AdminEvent Report Test Cases

Not all test cases within a spreadsheet are necessarily applicable to an SFR. That is, only a subset of the test cases in each spreadsheet is actually applicable to the evaluation. For spreadsheet items b and c above, only a very small number of test cases were relevant. These were executed by Lucent on LMF Version 3.0 and found to pass. Table 7 provides an indication of the number of functional tests performed by the developer that correspond directly to SFRs.

Table 7: Relevant Functional Test Cases

Spreadsheet	Applicable Requirement	# of Relevant Test Cases
1. LMF 3.0 Release Test Cases	FDP_IFC.1 FDP_IFF.1 FMT_MSA.3 FAU_GEN.1	~240 test cases
2. Test Cases for Download (Release 3.0)	FDP_IFC.1	~50 Test cases
3. LMF 3.0, non-IP Protocol Feature Test Cases	FDP_IFC.1	3 Test cases
4. Les Midouin – Test cases for Release 3.0	FIA_ATD.1 FIA_UID.2 FIA_UAU.1 FAU_GEN.1	~150 Test Cases
5. Lucent Managed Firewall AdminEvent Report Test Cases	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3	~50 test cases[4]

Many of the test cases contained within spreadsheets numbered a, d, and e were exercising TOE security functions of interest to the evaluation. However, even these spreadsheets contained significant numbers of tests that did not apply. For instance, many test cases described within the spreadsheets pertain to performance issues, the VPN features, and proper wording of error messages. Such test cases were ignored by the evaluation team.

[4] One of these test cases was very detailed, requiring the tester to actually perform over 50 individual tests to validate that every audit event type could be generated properly, and with accurate values.

The evaluation team performed a significant amount of independent testing to ensure that all security functional requirements had been tested. This included conducting tests for security functions that had already been tested by the LMF development team. In addition, the penetration testing effort required functional testing to be performed relating to the FDP_IFF and FDP_IFC requirements. Table 8 illustrates that between the developers and the evaluation team, all security functional requirements had been tested.

Table 8: Testing Coverage

Function Class	Identifier	Testing performed by
Security Audit	FAU.GEN.1	Developer, Evaluation Team
	FAU.SAR.1	Developer, Evaluation Team
	FAU.SAR.3	Developer, Evaluation Team
User Data Protection	FDP_IFC.1	Developer, Evaluation Team
	FDP_IFF.1	Developer, Evaluation Team
	FDP_RIP.2	Evaluation Team
Identification and Authentication	FIA_ATD.1	Developer, Evaluation Team
	FIA_UID.2	Developer, Evaluation Team
	FIA_UAU.1	Developer, Evaluation Team
Security Management	FMT_MOF.1	Evaluation Team
	FMT_SMR.1	Evaluation Team
	FMT_MSA.3	Developer
Protection of TOE Security Functions	FPT_RVM.1	Evaluation Team
	FPT_SEP.1	Evaluation Team
	FPT_STM.1	Evaluation Team

6.2 Functional Testing

Lucent performs functional testing of the LMF as part of their release cycle. Functional tests are defined and documented using a set of Excel spreadsheets. This documentation takes the form of an enumerated and individually identified set of test cases. That is, a line in a spreadsheet describes the test case and gives the test case a unique name.

Each spreadsheet is executed in a particular network configuration. Since none of these configurations equated to the evaluated configuration (as described by the [LMF_IGS]), the evaluation validated the vendor's testing against the evaluated configuration through independent testing of the LMF in an evaluated configuration.

This same spreadsheet is also used to track the results of testing. Therefore, along with the test case name and description are the test results, the name of the tester that performed the test, and "trouble reports/notes" pertaining to the test execution.

Finally, the team's observations were that testers often spend significant effort verifying that a testing environment is configured as expected. Testers maintain network diagrams which show the network topology, IP subnets, zones, and physical wiring of their testing environment. Prior to performing the functional tests described in a spreadsheet, the tester verifies this environment. The evaluation team observed that this validation process was effective.

The functional tests performed and documented by the developer did not completely cover all security functional requirements. Therefore, the evaluation team also tested the security functionality of the TOE as part of the Independent Testing (ATE_IND.2) assurance requirements.

6.3 Independent Testing

Lucent provided the evaluation team with the necessary hardware and software to create a testing network at the evaluation facility. The TOE was installed and configured as described in the [LMF_IGS] and [LMF_AGD] documents. In addition, the network was installed as illustrated in Figure 1.

The evaluation team used this testing network to validate the installation and configuration instructions in the IGS, to conduct team functional testing and to conduct vulnerability testing/analysis. Team functional testing took two forms. There was testing performed in the evaluation facility and observation of testing performed at the vendor's site.

The evaluation team performed a set of tests for each of the security functional requirements. This ensured that the combination of both the developer's tests and those performed by the evaluation team completely covered all security functional requirements. The testing coverage is illustrated in Table 8. The independent testing was concentrated in the following areas:

a) ***Installation and configuration.*** The evaluation team ensured that the installation and generation procedures resulted in secure configuration. This included testing that a restrictive configuration was installed by default.

b) ***Creation/Deletion/Modification of Traffic flow rules.*** This set of tests checked that an administrator could modify and set an information flow control security policy. The team spent considerable time checking that an installed security policy was correctly enforced by the TOE.

c) ***Verification of audit data creation and accuracy.*** The evaluation team ensured that the TOE was capable of creating all required audit records. This testing effort also verified that the correct information was recorded with each event and that the administrator could search and sort the audit records with the required attributes.

d) ***Verification that padding did not include residual data.*** The evaluation team derived a set of tests to ensure that residual data could not be transferred between sessions.

e) ***Creation and Use of system administration accounts.*** The evaluation team tested all functions of the creation of the administrator accounts.

f) ***Validation that traffic flow halts if auditing cannot be performed.*** Tests were created to ensure that the FA device halted firewall functions when it lost contact with the SMS.

g) ***Security Management.*** The evaluation team ensured that all security management functions specified in the [LMF_ST] operated as specified.

This testing effort was used to gain assurance that the TOE meets the requirements of the identified SFRs. The tests covered aspects of the security functional requirements that had not been tested by the developer as part of the functional testing of the TOE. In addition to testing at the evaluation facility, the evaluation team participated in testing at the vendor's facility. This testing effort was primarily concentrated on testing the enforcement of the information flow policy on traffic through the firewall. All tests performed by the evaluation team produced expected results and confirmed that the TOE implements all identified security functional requirements.

6.4 Penetration Testing

The [LMF_VA] document identified several potential vulnerabilities that may apply to products like the LMF. Many of these potential vulnerabilities and the associated analysis were drawn from Appendix A of the [TFF_PP]. Several of the vulnerabilities identified in both of these documents are not applicable to the LMF in the configuration evaluated, as noted below in Table 9. Table 9 provides a description of the set of potential vulnerabilities that were considered for applicability to the LMF in the configuration evaluated. The penetration testing effort concentrated on the remaining potentially applicable vulnerabilities to determine if any of the vulnerabilities were exploitable on the LMF in the configuration evaluated. The penetration testing effort did not identify evidence of exploitable vulnerabilities when the TOE was installed and configured as described in the [LMF_IGS] and [LMF_AGD] documents.

Table 9: Potentially Applicable Vulnerabilities

Vulnerability	Source	Description
FTP daemon vulnerabilities	[TFF_PP]	Not applicable – this problem is associated with the application layer.
Rlogin with term environment variable	[TFF_PP]	Not applicable - this problem is associated with the application layer.
Sendmail vulnerability	[TFF_PP]	Not applicable - this problem is associated with the application layer.
Telnet environment option	[TFF_PP]	Not applicable - this problem is associated with the application layer.
TFTP daemon attacks	[TFF_PP]	Not applicable - this problem is associated with the application layer.
Syslog vulnerability	[TFF_PP]	Not applicable - this problem is associated with the application layer.
IP spoofing attacks	[TFF_PP]	Possible vulnerability – addressed in the penetration testing phase of this work package.
UDP attacks	[TFF_PP]	Possible vulnerability – addressed in the penetration testing phase of this work package.
ICMP vulnerability	[TFF_PP]	Possible vulnerability – addressed in the penetration testing phase of this work package.
IP loose source route option	[TFF_PP]	Possible vulnerability – addressed in the penetration testing phase of this work package.
RIP vulnerability	[TFF_PP]	Not applicable
ARP vulnerability	[TFF_PP]	Possible vulnerability – addressed in the penetration testing phase of this work package.
DNS vulnerabilities	[TFF_PP]	Not applicable
Encryption vulnerabilities	[LMF_VA]	Not applicable – the TOE is not relying on encryption mechanisms to provide assurance.
Smurf – IP denial of service attacks	[LMF_VA]	Possible vulnerability – addressed in the penetration testing phase of this work package.

Vulnerability	Source	Description
Teardrop attack	[LMF_VA]	Possible vulnerability – addressed in the penetration testing phase of this work package.
LAND attack	[LMF_VA]	Possible vulnerability – addressed in the penetration testing phase of this work package.
Web access vulnerabilities	[LMF_VA]	Vulnerability testing demonstrated that SMS was isolated from networks mediated by the TOE.
Java Script vulnerability	[LMF_VA]	Vulnerability testing demonstrated that SMS was isolated from networks mediated by the TOE.
CGI bin vulnerability	[LMF_VA]	Vulnerability testing demonstrated that SMS was isolated from networks mediated by the TOE.
Httpd nph-test-cgi script	[LMF_VA]	Vulnerability testing demonstrated that SMS was isolated from networks mediated by the TOE.
Solaris vulnerabilities	[LMF_VA]	Not applicable – the evaluated configuration does not include the Solaris operating system.
X-Windows vulnerabilities	[LMF_VA]	Not applicable – the evaluated configuration does not include the Solaris operating system.

Therefore, the evaluation team addressed the following vulnerabilities:

a) IP spoofing attacks

b) UDP attacks

c) ICMP vulnerability

d) IP loose source route option

e) ARP vulnerability

f) Smurf – IP denial of service attacks

g) Teardrop attack

h) LAND attack

The penetration testing effort concentrated on the above-mentioned potential vulnerabilities. In addition, the team attempted many variations of these attack methods. The penetration team also performed a significant level of functional testing to provide assurance that the information flow security policy, defined in the [LMF_ST], is being correctly enforced by the LMF.

The penetration testing effort did not provide evidence of exploitable vulnerabilities when the TOE was installed and configured as described in the [LMF_IGS] and [LMF_AGD] documents.

7 Results of the evaluation

Section 7.1 provides a detailed description of the evaluator's findings for the assurance requirements that were addressed as a result of the work conducted for the EAL2 evaluation of the LMF. In addition, Section 7.2 provides an analysis of how the identified security functional requirements have been met by the TOE.

7.1 Security Assurance Requirements

Table 10 provides a listing of the security assurance requirements for the EAL2 level of assurance. The following sections provide a detailed summary of the evaluator's findings for each of these assurance classes.

Table 10: EAL2 Security Assurance Requirements

Assurance Class	Identifier	Description
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

7.1.1 Configuration Management

The EAL2 level of assurance requires that the following component be addressed for the Configuration Management assurance class:

a) ACM_CAP.2 Configuration items

ACM_CAP.2 Configuration items

The objective for the ACM_CAP.2 assurance family is to ensure that a unique reference is provided for the LMF and to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. The evaluator performed an analysis of the [LMF_CM] document to confirm that all requirements for content and presentation had been met.

The evaluation team was able to confirm that the LMF is labeled with its own reference and that the reference is unique for each version of the LMF. The [LMF_CM] also contained a configuration list, which described the configuration items that comprised the TOE. In addition, the [LMF_CM] document describes the method and system, used to uniquely identify the configuration items.

Verdict The TOE meets the requirements of ACM_CAP.2.

7.1.2 Delivery and Operation

The EAL2 level of assurance requires that the following components be addressed for the Delivery and Operation assurance class:

a) ADO_DEL.1 Delivery procedures

b) ADO_IGS.1 Installation, generation, and start-up procedures

ADO_DEL.1 Delivery procedures

The requirements for delivery call for system control and distribution facilities and procedures that provide assurance that the recipient receives the TOE that the sender intended to send, without any modifications. The evaluator performed an analysis of the [LMF_IGS] document to confirm that all requirements for content and presentation had been met.

The [LMF_IGS] document describes all procedures that are necessary to maintain security when distributing versions of the LMF to a customer's site. Through the [LMF_IGS] document, Lucent has provided a description of the delivery procedures for the LMF. In addition, the evaluation team was able to determine that the delivery procedures are being used.

Verdict The TOE meets the requirements of ADO_DEL.1.

ADO_IGS.1 Installation, generation, and start-up procedures

The installation, generation, and start-up procedures are required to ensure that the TOE can be installed, generated, and started up in a secure manner as intended by the developer. The requirements for installation, generation, and start-up call for a secure transition from the TOE's implementation representation being under configuration control to its initial operation in the customer's environment.

The evaluator performed an analysis of the [LMF_IGS] document to confirm that all requirements for content and presentation had been met. In addition, the evaluation team determined, by conducting the procedures, that the installation, generation, and start-up procedures resulted in a secure configuration.

The [LMF_IGS] document describes the steps necessary for secure installation, generation, and start-up of the LMF. Through analysis of the development documentation and functional testing of the LMF, the evaluation team identified several configuration settings and installation procedures that must be adhered to by the System Administrator to ensure that the SFRs are met by the product. These details have been captured in the [LMF_IGS] document to ensure that the LMF operates in a secure manner. Specific details relating to the procedures and configuration methods used to meet the SFRs of the [LMF_ST] are provided in Section 7.2 of this report, Security Functional Requirements. In addition, Section 2.1.2 of this report summarizes these procedures and configuration settings through the description of the evaluated configuration.

Verdict The TOE meets the requirements of ADO_IGS.1.

7.1.3 Development

The EAL2 level of assurance requires that the following components be addressed for the Development assurance class:

a) ADV_FSP.1 Informal functional specification

b) ADV_HLD.1 Descriptive high-level design

c) ADV_RCR.1 Informal correspondence demonstration

ADV_FSP.1 Informal functional specification

The functional specification is a high-level description of the user-visible interface and behavior of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed.

The evaluators performed an analysis of the [LMF_FSP] document to confirm that all requirements for content and presentation had been met. In addition, the evaluators determined that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Describing the TSF and its external interfaces in an informal style, the [LMF_FSP] was determined to be internally consistent. In addition, the [LMF_FSP] document provided a description of the purpose and method of use for all external TSF interfaces and details of effects, exceptions, and error messages. It was determined that the functional specification described in the [LMF_FSP] document completely represented the TSF.

The evaluation team was able to determine that the specification of the security functions in the [LMF_FSP] would produce a correct and complete instantiation of the TOE security functional requirements. Section 7.2 of this report describes how each of the SFRs, defined in the [LMF_ST], have been met by the LMF and provides further details relating to the evaluation team's analysis methods and findings.

Verdict The TOE meets the requirements of ADV_FSP.1.

ADV_HLD.1 Descriptive high-level design

The high-level design of a TOE provides a description of the TSF in terms of major structural units (i.e., subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the TOE provides an architecture appropriate to implement the TOE security functional requirements.

The high-level design refines the functional specification into subsystems. For each subsystem of the TSF, the high-level design describes its purpose and function and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design.

The evaluators performed an analysis of the [LMF_HLD] document to confirm that all requirements for content and presentation had been met. In addition, the evaluators determined that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

The [LMF_HLD] informally described the LMF's system architecture through a set of subsystems. The subsystems were supported by a description of the security functionality that each provided. In addition, the [LMF_HLD] described hardware and software that are used by the LMF to support the TSF.

The [LMF_HLD] identified all interfaces to the subsystems of the LMF and provided a detailed description of the purpose of these interfaces. The description identified which of these interfaces were externally visible.

The evaluation team determined that the described security functionality of the LMF's subsystems in the [LMF_HLD] would produce a correct and complete instantiation of the TOE security functional requirements. Section 7.2 of this report describes how each of the SFRs, defined in the [LMF_ST], have been met by the LMF and provides further details relating to the evaluation team's analysis methods and findings.

Verdict The TOE meets the requirements of ADV_HLD.1.

ADV_RCR.1 Informal correspondence demonstration

The correspondence between the various TSF representations addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

The demonstration of correspondence was provided through the [LMF_FSP] and the [LMF_HLD]. Therefore, the evaluators performed an analysis of these documents to confirm that all requirements for content and presentation had been met.

The evaluation team confirmed that a correspondence exists between each adjacent pair of TSF representations and that the security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract representation. Therefore, correspondence could be determined between the TOE Summary Specification in the [LMF_ST] to the security functionality identified in the [LMF_FSP] and finally to the subsystems identified in the [LMF_HLD].

Verdict The TOE meets the requirements of ADV_RCR.1.

7.1.4 Guidance Documents

The EAL2 level of assurance requires that the following families be addressed for the Guidance Documents assurance class:

a) AGD_ADM.1 Administrator guidance

b) AGD_USR.1 User guidance

AGD_ADM.1 Administrator guidance

The administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. Because the secure operation of the TOE is dependent upon the correct performance of the TSF, persons responsible for performing these functions are trusted by the TSF. Administrator guidance is intended to help administrators understand the security functions provided by the TOE, including both functions that require the administrator to perform security-critical actions and those functions that provide security-critical information.

The evaluators performed an analysis of the [LMF_AGD] document to confirm that all requirements for content and presentation had been met. The [LMF_AGD] document was used to provide a concise set of security relevant references to the vendor-supplied installation and administrator guidance documents. The vendor supplied the [LMF_SAR], the [LMF_BIG], and the [LMF_IG], which are identified in Section 5 of this report.

The evaluators confirmed that the [LMF_AGD] document described the administrative functions and interfaces available to the administrator of the LMF and that guidance was provided in how to use these interfaces to securely administer the LMF. The guidance documents provide adequate warnings and cautions relating to certain administrative tasks.

It was determined that the information contained in the entire set of administrative documentation covered all security parameters that are under the control of the administrator and that secure values for these parameters are provided where appropriate. In addition, it was determined that the administration documentation was consistent with other deliverables that were supplied to the evaluation team.

The [LMF_AGD] document is designed to be used in conjunction with the [LMF_IGS] document for the administrator to not only administer the LMF in a secure manner but also have the product installed and initially configured in a way that the requirements of the [LMF_ST] are met. The [LMF_IGS] document provides a detailed description of the required operating environment.

Verdict The TOE meets the requirements of AGD_ADM.1.

AGD_USR.1 User guidance

The LMF does not allow general users to interact directly with the security functionality of the TOE. Therefore, there is no requirement to provide any user documentation, and an analysis of this set of requirements is unnecessary.

Verdict Not applicable.

7.1.5 Testing

The EAL2 level of assurance requires that the following families be addressed for the Guidance Documents assurance class:

a) ATE_COV.1 Evidence of coverage

b) ATE_FUN.1 Functional testing

c) ATE_IND.2 Independent testing – sample

ATE_COV.1 Evidence of coverage

The objective of this component is to establish that the TSF has been tested against its functional specification. This is to be achieved through an examination of developer evidence of correspondence.

The evaluators performed an analysis of the LMF test case descriptions available in the form of Excel spreadsheets. These spreadsheets enumerate the test cases performed by testers, and record the results of each test case. The evaluation team verified that tests identified in the testing documentation corresponded to security functional requirements. The work performed for this assurance requirement is further discusses in Section 6.1, Testing Coverage.

The evaluation team performed additional functional testing to ensure that all security functions had been completely tested. Table 8 in Section 6.1, Testing Coverage, identifies all security functional requirements and provides an indication of those that were tested by the developer and those that had additional testing performed by the evaluation team. The result was that all security functional requirements were tested by either the developers or the evaluation team.

Verdict The TOE meets the requirements of ATE_COV.1.

ATE_FUN.1 Functional testing

The objective of this component is to determine that all security functions perform as specified. The developer is required to perform testing and to provide test documentation.

The evaluators performed a review of the Lucent test case documentation to ensure that Lucent tested all relevant test cases identified during the ATE_COV.1 analysis on LMF Version 3.0. The evaluators found that all relevant tests were executed and functioned as expected. A more detailed description of the evaluators analysis is provided in Section 6.2, Functional Testing.

Table 8 in Section 6.1,Testing Coverage, illustrates that some of the security functional requirements of the TOE were not completely tested by the development team. Therefore, the evaluation team conducted a set of tests to provide complete testing coverage of the security functional requirements.

Verdict The TOE meets the requirements of ATE_FUN.1.

ATE_IND.2 Independent testing – sample

The objective is to determine that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests. In addition, if the testing of the security functional requirements is incomplete, the evaluation team is required to perform additional functional testing to ensure adequate testing coverage.

The evaluation team reviewed the testing documentation supplied for the ATE_FUN.1 requirements. The evaluation team conducted some of these tests at the CSC evaluation facility and on site using the developer's test environment.

The evaluation team constructed a testing environment within the evaluation facility. This test platform was used during the evaluation team's functional and vulnerability testing. The evaluation team installed and configured the TOE as described in the [LMF_IGS] and [LMF_AGD] documents. This environment was used to perform functional testing to confirm the developer's test results. The independent testing was concentrated in the following areas:

a) ***Installation and configuration.*** The evaluation team ensured that the installation and generation procedures resulted in secure configuration. This included testing that a restrictive configuration was installed by default.

b) ***Creation/Deletion/Modification of Traffic flow rules.*** This set of tests checked that an administrator could modify and set an information flow control security policy. The team spent considerable time checking that an installed security policy was correctly enforced by the TOE.

c) ***Verification of audit data creation and accuracy.*** The evaluation team ensured that the TOE was capable of creating all required audit records. This testing effort also verified that the correct information was recorded with each event and that the administrator could search and sort the audit records with the required attributes.

d) ***Verification that padding did not include residual data.*** The evaluation team derived a set of tests to ensure that residual data could not be transferred between sessions.

e) ***Creation and Use of system administration accounts.*** The evaluation team tested all functions of the creation of the administrator accounts.

f) ***Validation that traffic flow halts if auditing cannot be performed.*** Tests were created to ensure that the FA device halted firewall functions when it lost contact with the SMS.

g) ***Security Management.*** The evaluation team ensured that all security management functions specified in the [LMF_ST] operated as specified.

All tests performed by the evaluation team produced expected results and confirmed that the TOE implements all identified security functional requirements. Table 8 identifies the security functional requirements tested by the evaluation team.

Verdict The TOE meets the requirements of ATE_IND.2.

7.1.6 Vulnerability Assessment

The EAL2 level of assurance requires that the following families be addressed for the Vulnerability Assessment assurance class:

a) AVA_SOF.1 Strength of function evaluation

b) AVA_VLA.1 Developer vulnerability analysis

AVA_SOF.1 Strength of function evaluation

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For these functions, a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.

The [LMF_ST] specifies that a strength of function claim is made for the password mechanism used by the LMF to meet the FIA_UAU.1 requirement. The evaluators performed an analysis of the password mechanism of the SMS host operating system and not the mechanism provided by the SMS software. This decision was made as the password mechanism of the SMS host operating system is used to protect the SMS.

The claim is that the probability of the authentication data can be guessed is no greater than one in one million. The strength of function analysis performed by the evaluators determined that the password policy set by the [LMF_IGS] document ensured that the strength of function claim was correct.

Verdict The TOE meets the requirements of AVA_SOF.1.

AVA_VLA.1 Developer vulnerability analysis

A vulnerability analysis was performed by the developer to ascertain the presence of obvious security vulnerabilities and to confirm that they cannot be exploited in the intended environment for the TOE.

The evaluation team performed an analysis of the [LMF_VA] document to determine if the vulnerabilities could be exploited in the intended environment. In addition, the evaluation team built on the developer's vulnerability analysis and performed a significant level of penetration testing to confirm that the vulnerabilities identified in Appendix A of the [TFF_PP][5] could not be exploited in the intended environment. The penetration testing team used input provided from analysis performed as part of the functional testing and design analysis of the LMF. A more detailed description of the penetration testing is provided in Section 6.4, Penetration Testing.

[5] The developers used Annex A of the [TFF_PP] as a basis for the Vulnerability Analysis. However, the Vulnerability Analysis also identified several other potential vulnerabilities that were not included as part of [TFF_PP] Annex A.

The testing team concentrated efforts in determining if the LMF correctly enforced the requirements of the information flow control security policy. The testing team was able to confirm that the LMF correctly enforced the security policy when configured as stated in the [LMF_IGS] document. The team determined that the TOE is resistant to penetration attacks that could be performed by an attacker possessing a low attack potential

Verdict The TOE meets the requirements of AVA_VLA.1.

7.2 Security Functional Requirements

This section provides a summary of the evaluation team's findings relating to the accurate and complete instantiation of the SFRs identified in the [LMF_ST]. The information provided here has been predominantly derived from analysis performed for the development and testing classes of assurance.

Table 11 provides a listing of the set of security functional requirements that the LMF is required to meet.

Table 11: Security Functional Requirements

Function Class	Identifier	Description
Security Audit	FAU.GEN.1	Audit data generation
	FAU.SAR.1	Audit review
	FAU.SAR.3	Selectable audit review
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_RIP.2	Full residual information protection
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UID.2	User identification before any action
	FIA_UAU.1	Timing of authentication
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_SMR.1	Security Roles
	FMT_MSA.3	Static attribute initialization
Protection of TOE Security Functions	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_STM.1	Reliable time and date stamps

7.2.1 FDP_IFC.1 – Subset information flow control

This requirement specifies an information flow control Security Function Policy (SFP) which controls the passing or dropping (operation) of traffic (information) between external IT entities (subjects) from either an internal or an external network.

The LMF has been designed to enforce an information flow control security policy. The System Administrator is able to design and implement an organization's information flow control security policy through the SMS GUI interface. This policy is downloaded from the SMS to the FA device via a communications link.

The development documentation specifies the characteristics of the security policy. The subjects of the policy are defined as external IT entities that are able to pass traffic through the FA device. The subjects (external IT entities) are identified by their associated IP address. Therefore, a subject of the security policy must provide information to the FA device in the form of an IP datagram.

The LMF will then either ***PASS*** or ***DROP*** the information according to the specified rules of the security policy. The IP datagram is examined by the LMF to determine if its characteristics match the values set by the System Administrator through the security policy.

The LMF will only allow a decision to be performed on traffic with characteristics that can be mapped to security attributes specified in the FDP_IFF.1 requirement. Therefore, the FA device will drop information that does not contain the defined security attributes.

Conclusion The TOE meets the requirements of FDP_IFC.1.

7.2.2 FDP_IFF.1 Simple security attributes

This SFR identifies the security attributes, for both the subject and the information, which will be used to enforce the SFP.

Through analysis performed for the testing and development assurance classes, the evaluation team was able to determine that the following security attributes can be used to enforce the information flow security policy:

a) ***Source IP address***. The LMF can use the source IP address contained in the IP datagram to enforce the security policy. This address is defined as the subject's security attribute that must be used to enforce the security policy. This address is used to identify the subject. The source IP address can be used to enforce a rule set through a zone security policy.

b) ***Destination IP address***. This attribute can be used to enforce the security policy and is defined as the presumed address of the destination subject. The destination IP address can be used to enforce a rule set through a zone security policy.

c) ***TCP or UDP port number***. A set of services are related to the TCP or UDP port number and these can be defined through the Services Group function and then applied to a zone security policy.

d) ***Physical Ethernet port***. The LMF uses these attributes to define zone security policies, which are applied to a physical network interface on the FA. The zone security policies are defined through the association of a rule set that is defined by Host and Service Groups. A Host Group is used to identify a set of IP addresses and a Service Group is used to define a set of services through its port number and associated transport layer protocol. Therefore, the System Administrator can use these predefined groups to create the rules that will enforce the policy. These zone policies are associated to particular physical network interfaces.

e) ***Transport Layer Protocol***. The SMS allows the System Administrator to define the transport layer protocol as a service group, which can be applied to a zone security policy.

The FDP_IFF.1.2 and FDP_IFF.1.6 components of this requirement, explicitly state several cases where an information flow shall be passed or denied. Each of the stated requirements for these components is addressed in the following paragraphs.

The FDP_IFF.1.2a component provides the following requirement statements that address cases where subjects on an internal network are able to cause information to flow through the TOE to another connected network:

a) *All the information security attribute values are unambiguously permitted by the information flow security policy rules*. The development documentation describes a decision making process that complies with this statement. In addition, the functional testing performed by the developer and evaluation team supports this statement.

b) *The presumed address of the source subject, in the information, translates to an internal network address*. The development documentation identifies address validation as a process performed by the FA decision module subsystem. This is described as verifying that Ethernet packet source address could only originate on the physical interface where the packet was received. In addition, the [LMF_IGS] document identifies a set of rules designed to enforce this security policy, and the System Administrator is required to implement these rule sets to ensure that this requirement has been met. These rule sets are described in full detail in Section 2.1.2.2 of this report.

c) *The presumed address of the destination subject, in the information, translates to an address on the other connected network.* See commentary provided for requirement described in paragraph b above.

The FDP_IFF.1.2b component provides the following requirement statements that address cases where subjects on an external network are able to cause information to flow through the TOE to another connected network:

a) *All the information security attribute values are unambiguously permitted by the information flow security policy rules*. The development documentation describes a decision making process that complies with this statement. In addition, the functional testing performed by the developer and evaluation team supports this statement.

b) *The presumed address of the source subject, in the information, translates to an external network address.* See commentary provided for requirement described in paragraph b above.

c) *The presumed address of the destination subject, in the information, translates to an address on the other connected network*. See commentary provided for requirement described in paragraph b for the FDP_IFF.1.2a component.

The requirements of FDP_IFF.1.6 provide several cases where an information flow shall be explicitly denied. A description for each of these requirements is provided as follows:

a) *The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.* See commentary provided for requirement described in paragraph b for the FDP_IFF.1.2a component.

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.* See commentary provided for requirement described in paragraph b for the FDP_IFF.1.2a component.

c) *The TOE shall reject requests for access or services where the information arrives on either an internal or external interface, and the presumed address of the source subject is an external IT entity on a broadcast network.* The development documentation does not describe this functionality. Therefore to meet this requirement, the [LMF_IGS] document identifies a set of rules designed to enforce this requirement, and the System Administrator is required to implement these rule sets to ensure that this requirement has been met. This rule set is described in full detail in Section 2.1.2.2 of this report.

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.* See commentary provided for the requirement described in paragraph c above.

Conclusion The TOE meets the requirements of FDP_IFF.1.

7.2.3 FDP_RIP.2 Full residual information protection

This requirement addresses the need to ensure that information from previous network sessions is no longer accessible. This requirement provides protection for information that has been logically deleted or released, but may still be present in the TOE.

The development documentation describes the mechanisms used to ensure that residual information is not transferred to a following session. The description indicates that pointers are used by the FA code to determine the beginning and end of a packet that is being stored in memory. The description states that *"the correct operation of these pointers ensures that data previously stored in memory is not inadvertently included in packet."*

This description of this mechanism raised concerns that this may not be a highly effective method for ensuring that residual data is not transferred. Therefore, the work performed for the vulnerability assessment assurance class was used to further scrutinize the effectiveness of this mechanism to meet the FDP_RIP.2 requirement. The testing performed by the evaluation team determined that the LMF was correctly managing residual data.

Conclusion The TOE meets the requirements of FDP_RIP.2.

7.2.4 FMT_MSA.1 Static attribute initialization

This SFR is used to provide restrictive initial or default values to the security attributes of the subject and information. This will provide a restricted security policy before adjustments are made by the authorized administrator to reflect the organization's network architecture and security policy.

The default values are meant to be restrictive so that the TOE denies inbound information until the authorized administrator modifies the default values. There are several occasions when the LMF is required to provide a default state for the information flow security policy.

When the System Administrator first creates a new policy through the SMS, the initial set of values provide a ***deny all*** policy. The System Administrator must then manipulate the rules to create a set of zone policies, which reflect the organization's information flow security policy.

When a System Administrator creates a new FA, two default zones are automatically associated with the device. The purpose of these zones is to protect the SMS and the FA by providing a set of default host groups, service groups, and security rules. These zones define the set of services, which the SMS and FA use to communicate and the rules that will restrict that communications channel.

When the FA is first started and it has not been configured by a bootable floppy from the SMS, it will not have an operating system and therefore does not have the ability to process traffic. In addition, if the FA is rebooted and is unable to connect to the SMS then it will fail to the ***deny all*** state.

Conclusion The TOE meets the requirements of FMT_MSA.1.

7.2.5 FPT_STM.1 – Reliable time stamps

The Logger subsystem operates within the SMS. It receives audit data from other SMS subsystems and from the Audit Module within the FA. The Logger subsystem saves received audit data into two logs: an Events Log and a Session Log. The Event log contains audit data pertaining to activity on the SMS. The session log contains audit data pertaining to sessions that are permitted or denied by the FA. The session log contains audit data only from the audit module within the FA. The Logger subsystem places its own time stamp on all audit data that is placed into the Event log and the Session log. No other timestamp appears within audit data.

The Logger subsystem, the other SMS subsystems and the Audit Module within the FA, cooperate to place audit events into the appropriate logs in an appropriate order. First, the Logger subsystem is simply invoked by the other SMS subsystems when audit events occur. Thus, the Logger subsystem places audit records from other SMS subsystems into the logs in the order in which the other subsystems generate the audit records. The audit records received from the FA each possess a timestamp written by the FA. This timestamp along with the network protocol (TCP) is used to ensure that audit records from the FA are written into the logs in the same order in which the audit module of the FA generates events. This ordering approach, however, could not guarantee proper sequencing if multiple FAs were used. Thus, the evaluated configuration, as described by [LMF_IGS], permits only a single FA.

This implementation satisfies the requirement because the activity occurring at each physical component gets saved in the audit trail in the order in which the events occur. The timestamp, applied to every record, sequences the audit events based upon the order in which the Logger subsystem receives the audit event.[6]

Conclusion The TOE meets the requirements of FPT_STM.1.

[6] Any change on the SMS, that causes a change in behavior for the FA, will appear in the SMS logs before any session audit records affected by that change.

7.2.6 FAU_GEN.1 – Audit data generation

This requirement is used to identify the auditable events for which audit records should be generated, and the information to be provided in the audit records.

This requirement provides a set of auditable events for which the LMF must produce an audit record. The [LMF_ST] identifies several events that must be audited and the implementation of each is described as follows:

a) ***Start-up and shutdown of the audit functions***. The LMF produces an audit record when the audit services have been started. This event is written to the Admin Events Log. When the FA device has lost contact with the SMS an audit event is also produced that indicates the audit services have been lost or shut down. The [LMF_IGS] document provides procedures for configuring the SMS host operating system to audit the shutdown of the audit functions on the SMS.

b) ***Modification to the group of authorized administrators***. The LMF produces an audit record and it is stored in the Admin Events Log. The record includes the action performed and the account that is modified. The [LMF_IGS] provides procedures for configuring the SMS host operating system to record an audit event when the group of administrator's accounts is modified on the host operating system.

c) ***All use of the user identification mechanism, including the user identity provided***. The SMS audits all successful and failed identification and authentication attempts and stores the record in the Admin Events Log. The user's identity is provided in the audit record. The [LMF_IGS] provides procedures for configuring the SMS host operating system to audit these events.

d) ***Any use of the authentication mechanism***. The SMS audits all successful and failed attempts to use the SMS login mechanism. The SMS stores the audit record in the Admin Events Log and the user identity is recorded with the event. The [LMF_IGS] provides procedures for configuring the SMS host operating system to audit these events.

e) ***The reaching of the threshold for unsuccessful authentication attempts***. The LMF is not required to perform this function, as it does not provide general user accounts and it is not practical to lock out the System Administrator's account. It is stated in [CC_PART2A] that *"in order to prevent denial of service, TOE's usually ensure that there is at least one user account that cannot be disabled."* This is important for the LMF's System Administrator account.

f) ***Restoration by the authorized administrator of the user's ability to authenticate***. See description for item e above.

g) ***All decisions on requests for information flow***. The LMF audit module produces an audit record for successful and unsuccessful session attempts. The audit record is stored in the Session Log and includes the action taken by the FA (pass or drop).

h) ***Changes to the time***. The LMF does not audit changes to the time for either the SMS host or the FA device. Therefore, to meet this requirement a set of procedures is included in the [LMF_IGS] that describe how to configure the SMS host operating system to audit changes to the time.

i) ***Access to the audit trail***. The [LMF_IGS] provides procedures for configuring the SMS host operating system to audit access to the audit files.

The FAU_GEN.1.2 component requires that a minimum set of information be recorded with each audit record. The LMF provides a Session log file and an Administrative Event log file. There are several variations of both, but the general format is as follows:

a) Administrative Events Log

firewall_name : hhmmss : zone : event_description : administrator_id

b) Session Log

firewall_name : hhmmss : zone:direction : source_host : destination_host : protocol : source_port : destination_port : action : received_interface : sending_interface : alarm_code:rule_no

It is a requirement that the following information be recorded with each audit record:

a) ***Date and time of the event***. The Session and Admin Events Logs both record a timestamp with the event.

b) ***Type of event***. The Administrative Event Log Report provides an event description for each of the different types of audit records stored in this file. The session log files are recording only one type of event; therefore, it is not required to identify this as a separate field.

c) ***Subjects identities***. The session log files provide both the source and destination address of the subjects involved in the auditable event. The Admin Event Log provides the System Administrator's identification to associate administrative events to a specific administrator.

d) ***Outcome (success or failure)***. The session log file identifies *"action"* as an information field. This indicates that the packet will either be passed or dropped which would indicate either a success or failure.

When a modification is made to the group of users who are part of the authorized administrator's role, it is a requirement that the user identity being modified is recorded with the associated audit record. The LMF provides the following audit records relating to the modification of the administrator's group:

a) Add Administrator Account

source : hhmmss : event_description : administrator_id : new_admin

b) Modify Administrator Account

source : hhmmss : event_description : administrator_id : old_admin : new_admin

c) Delete Administrator Account

source : hhmmss : event_description : administrator_id : old_admin

Conclusion The TOE meets the requirements of FAU_GEN.1.

7.2.7 FAU_SAR.1 – Audit Review

This requirement provides the System Administrator with the capability to obtain and interpret the audit data in a human understandable format.

The System Administrator is able to review all data stored in both the Session and Admin Events log files. The SMS provides the System Administrator with a *"report wizard"* tool that provides the ability to create and memorize report formats. This provides the audit data in a human readable format and allows the System Administrator to filter and sort the audit data.

Conclusion The TOE meets the requirements of FAU_SAR.1.

7.2.8 FAU_SAR.3 – Selectable audit review

This requirement provides the System Administrator with the ability to perform searches and sorts on the audit files produced by the LMF.

The LMF provides an extensive, highly configurable report-generating function. This function provides a *"report wizard"* that allows the System Administrator to configure and view the audit logs in a number of different ways.

To meet the requirement, the System Administrator must be able to search and sort audit data based on the presumed subject address, range of dates, ranges of times, and ranges of addresses. The LMF provides the capability to perform all of these searches and sorts. In addition, the audit records can be searched and/or sorted on any of the fields that make up the complete audit records. The tool provides a full text search and the ability to filter out fields that the System Administrator may not want to view.

Conclusion The TOE meets the requirements of FAU_SAR.3.

7.2.9 FIA_ATD.1 – User attribute definition

This requirement defines the security attributes that are associated with users to support the TSP. To meet this requirement, an identity must be associated with a user, and a human user must be associated with the System Administrator role.

The SMS maintains the account information for the System and Zone Administrators of the TOE. The Remote Administration Daemon is a subsystem within the SMS that maintains the user identification and password of all accounts that exist within the SMS. In addition, the subsystem manages the information relating to the domain, privileges, and security role of the account.

The identities provided for each administrator account must be unique, allowing for accountability. In addition, the [LMF_IGS] document states that a corresponding account must be produced for the SMS host operating system. This account will also have a corresponding user identity and will be a part of the administrators group.

Conclusion The TOE meets the requirements of FIA_ATD.1.

7.2.10 FIA_UID.2 – User identification before any action

This requirement defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification. The users of the LMF include both System Administrators and external IT entities.

The decision module, located on the FA device, inspects traffic as it arrives on the external interfaces. The traffic is received by the FA from external IT entities. This information contains a unique IP source address, which is used by the LMF to identify the external IT entity. No other action is able to take place until the identification of the external IT entity has been determined.

The System Administrator is able to view the log files and other system files located on the SMS before having to identify them through the SMS identification and authentication mechanism. However, the [LMF_IGS] document states that each SMS System Administrator must have a corresponding SMS host operating system account. This ensures that each System Administrator will be identified by the SMS host operating system before allowing any other TSF mediated actions on behalf of that user.

Conclusion The TOE meets the requirements of FIA_UID.2.

7.2.11 FIA_UAU.1 Timing of authentication

This requirement identifies functions that are able to occur before a user is authenticated. This requirement identifies passing or dropping of traffic and identification of the user as the two functions that the LMF is able to perform on behalf of the user without requiring authentication.

Therefore, System Administrators are only able to identify themselves before authentication must occur if they wish to perform any other function. However, functional testing of the LMF revealed that once a System Administrator had access to the SMS host, there were a number of security related functions that the System Administrator could perform without authenticating through the SMS identification and authentication mechanism. Therefore, the [LMF_IGS] document mandates that each SMS System Administrator must have a corresponding account for the SMS host operating system, which ensures that authentication must take place before any other TSF mediated action.

The LMF is able to pass or drop traffic without having to authenticate the associated external IT entity. This allows the FA device to perform its firewall functionality without requiring each external IT entity, associated with a session, to authenticate. The only requirement is that these external IT entities are identified through the associated IP address.

Conclusion The TOE meets the requirements of FIA_UAU.1.

7.2.12 FMT_SMR.1 – Security roles

This requirement is used to define the administrator role and to associate a human user with that role.

The role of the authorized administrator is managed by the RAD subsystem within the SMS. The SMS stores the account information, and a unique identification must be provided for each of the administrators. This ensures that an individual can be associated with each of the System Administrator accounts. The LMF permits two categories of system administrators, which have different levels of privileges.

The System Administrator role is the most privileged type of account, and this user can perform all restricted tasks. A System Zone Administrator role is also identified, and this role allows the network to be divided into security zones. This administrator is only able to perform restricted operations for their defined security zone.

Conclusion The TOE meets the requirements of FMT_SMR.1.

7.2.13 FMT_MOF.1 Management of security function's behavior

This requirement identifies several security functions that must be restricted to the authorized administrator.

The security management functions of the LMF are performed by the System Administrator through the SMS. There are no general user accounts on the SMS, and the identification and authentication functionality ensures that the security management functions are restricted to the System Administrator. In addition, the FA and SMS will be installed in a physically secure environment.

The requirement states that the following functions must be provided and restricted:

a) ***Start-up and shutdown***. The evaluated configuration, as specified in the [LMF_IGS] and this document, has both the SMS and the FA in a physically secure operating environment. Therefore, this function will be restricted to the System Administrator.

b) ***Editing of security policy rules***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to create, delete, modify, and view information flow security policy rules that permit or deny information flow. It is clear that this functionality is both provided and restricted to the System Administrator.

c) ***Managing the user attribute values***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to create, delete, modify, and view user attributes associated with System Administrator accounts. It is clear that this functionality is both provided and restricted to the System Administrator.

d) ***Modifying and setting the threshold for authentication failure attempts***. This security management function is not relevant to this TOE.

e) ***Restoration of authentication capabilities***. This security management function is not relevant to this TOE.

f) ***External IT entities communicating with the TOE***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to enable and disable external IT entities from communicating with the FA device. The FA has a predefined rule set assigned to the FA device itself. This rule set is automatically created to enable only communications with the SMS host. It is clear that this functionality is both provided and restricted to the System Administrator. The evaluated configuration has the SMS on a physically and logically isolated network, and remote administration will be disabled.

g) ***Modification of the time and date***. When the FA device is first booted, the System Administrator is able to enter the system bios and modify the time and date settings for that device. This security management function is restricted to the System Administrator as the FA and SMS will be installed in a physically secure operating environment. The modification of the time and date on the SMS host is performed through the host operating system. This security management function is also protected by the identification and authentication mechanisms supplied by the host operating system.

h) ***Managing the audit trail***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to archive, create, delete, empty, and review the audit trail. It is clear that this functionality is both provided and restricted to the System Administrator.

i) ***Backup***. The operating system of the SMS host provides this security management function. The [LMF_IGS] document provides procedures and guidance on how to configure this function.

j) ***Recovery from backup***. The operating system of the SMS host provides this security management function. The [LMF_IGS] document provides procedures and guidance on how to configure this function.

k) ***Applying information flow security policy rules***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to apply information flow security policy rules that permit or deny information flows. It is clear that this functionality is both provided and restricted to the System Administrator.

l) ***Maintaining security zones***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to create, update, save, delete, and view a security zone, assign it to an interface, and load the assignment information onto the FA device.

m) ***Maintaining Host Groups***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to create, update, delete, and view Host Groups. A Host Group can then be applied to a security policy, which can then be assigned to a security zone.

n) ***Maintaining Service Groups***. This functionality is performed by the System Administrator through the SMS. The System Administrator has the ability to create, update, delete, and view Service Groups. A Service Group can then be applied to a security policy, which can then be assigned to a security zone.

Conclusion The TOE meets the requirements of FMT_MOF.1.

7.2.14 FPT_RVM.1 – Non-bypassability of the TSP

This requirement is used to ensure that any security enforcement function that is required to enforce the TSP is invoked and succeeds before the functions of the TSC can proceed. This TOE has only one SFP, information flow control policy, that was defined through the FDP_IFC.1 and FDP_IFF.1 SFRs. This SFP is the only policy that has been defined for this TOE and is therefore the TOE's TSP.

Therefore to meet the requirement, all data that arrives on the FA's physical interfaces must have the security attributes, identified in *FDP_IFF.1,* analyzed for conformance to the information flow security policy. That is, all information attempting to pass through the FA device must always invoke the LMF's Decision Module.

The information flow security policy requires that any information arriving on any of the network interfaces, which does not have the required security attributes identified in the *FDP_IFF.1 Simple security attributes* SFR, must be dropped. The characteristics of the information must allow that the decision module can make a decision as to either pass or drop the information. If the information does not have the required security attributes, then it must be dropped.

The development documentation provides a detailed description of the access control processing and the mechanisms used to make a decision to either pass or drop traffic. This description identifies the steps that the decision module takes in determining if data is allowed to pass. It is evident from this documentation that badly formed packets or traffic that do not comply with the specification are dropped.

However, the development documentation identifies a specific problem relating to the processing of ARP frames. ARP frames are transferred through the LMF without invoking the decision module. The ARP frames are required to be passed through the LMF so the FA can operate as a bridge device. An ARP frame can not be subjected to the security policy, as it does not have the security attributes required by the decision module.

Therefore, to meet this requirement, the LMF must provide a configuration that will disable the transfer of ARP. This configuration is described in the [LMF_IGS] document and identifies the need to assign an IP address for each of the network interface cards. In addition, each of the assigned IP addresses must be associated with a separate subnet. This will have the LMF working at the network layer and therefore operating as a traditional traffic filtering firewall. This ensures that the ARP frame is not passed through the FA device.

Thus, when the FA is configured as stated in the [LMF_IGS] document, the firewall's decision module is invoked to process all traffic through the FA.

Conclusion The TOE meets the requirements of FPT_RVM.1.

7.2.15 FPT_SEP.1 – TSF domain separation

This requirement is used to protect the TOE from external interference and tampering by untrusted subjects. To ensure domain separation, it is important that untrusted external IT entities are unable to perform or execute any process on the firewall.

The only IT entity allowed to communicate directly with the TOE is the SMS. The SMS is considered to be an internal IT entity as it is part of the TOE. However, it is important that trust is established between the FA and SMS, as the SMS is physically separate from the FA device. A problem could exist if an untrusted external IT entity was able to impersonate the management server. Thus, the evaluated configuration described in the [LMF_IGS] document mandates that the FA and SMS share a private LAN and that the defined rule set allows only administration activity on that LAN.

The RAD subsystem provides a trusted channel between the SMS and the Application Module subsystem of the FA device. The LMF uses encryption and authentication mechanisms to secure the SMS to FA communications. The RAD subsystem performs Diffie-Hellman for key exchange and triple DES for session encryption between the FA and SMS. In addition, ElGamal is used to provide digital signature functionality for the authentication mechanism. However, the evaluation is not relying upon these cryptographic mechanisms to authenticate the SMS and FA.

The LMF receives information from untrusted external IT entities on the FA's network interfaces. The traffic arrives on the network interfaces in the form of Ethernet frames These frames are unable to execute or perform any process on the firewall. The FA will only make a decision to either pass or drop the information according to a security policy that defines the type of information allowed to pass through the firewall. Therefore, there are no processes on the FA device that will allow the execution of data passed from untrusted external IT entities.

The memory management techniques and supporting hardware of the TOE ensure that the TSP of the TOE executes in a domain of its own. Information and processes received from external IT entities are unable to execute processes in that domain. Processes executed in response to the receipt of information from external IT entities are handled as separate processes and they cannot interfere with other processes being managed by the TOE. These arguments were supported by both functional and vulnerability testing performed by the evaluation team.

Conclusion The TOE meets the requirements of FPT_SEP.1.

8 Evaluator comments

The evaluation team was able to confirm that the Lucent Managed Firewall Version 3.0 meets the security assurance requirements for the Common Criteria EAL2 level of assurance. This implies that the product meets the security functional requirements as stated in the [LMF_ST].

It is important that the product is installed and configured as described in the [LMF_IGS] document and that administrators follow the guidance for secure operation of the TOE as described in the set of administration documentation.

9 Glossary

ARP	Address Resolution Protocol
CC	Common Criteria
CEM	Common Evaluation Methodology
CSC	Computer Sciences Corporation
DMZ	De-Militarized Zone
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
FA	Firewall Appliance
FER	Final Evaluation Report
IP	Internet Protocol
LAN	Local Area Network
LMF	Lucent Managed Firewall
NSA	National Security Agency
NIST	National Institute of Science & Technology
OR	Observation Report
PP	Protection Profile
SFR	Security Functional Requirements
SMS	Security Management Server
TCP	Transport Control Protocol
TCSEC	Trusted Computer Systems Evaluation Criteria
TEF	TTAP Evaluation Facility
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions

10 Bibliography

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated May 1998, Version 2.0

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated May 1998, Version 2.0

[CC_PART2A] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated May 1998, Version 2.0

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated May 1998, Version 2.0

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, Version 0.6

[LMF_AGD] Lucent Managed Firewall Administrator Guidance, Version 1.0, dated December 1998

[LMF_BIG] Lucent Managed Firewall Brick Installation Guide, Version 3.0, dated November 1998

[LMF_CM] Lucent Managed Firewall Version 3.0 Configuration Management, Version 2.3, dated 10/28/98

[LMF_FSP] Lucent Managed Firewall Version 3.0 Functional Specification, Version 1.1, dated 11/16/98

[LMF_IG] Lucent Managed Firewall Installation Guide, Version 3.0, dated November 1998.

[LMF_IGS] Lucent Managed Firewall Installation, Generation and Start-up, Version 8.0, dated November 1998

[LMF_SAR] Lucent Managed Firewall System Administrator Reference Manual, Version 3.0, dated November 1998

[LMF_ST] Lucent Managed Firewall Version 3.0 Security Target, Version 1.3, dated 22 December 1998

[LMF_HLD] Lucent Managed Firewall Version 3.0 High Level Design, Version 1.1, dated 11/30/98

[LMF_VA] Lucent Managed Firewall Version 3.0 Vulnerability Assessment, Version 1.0, dated 11/30/98

[TFF_PP] U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, dated November 1998, Version 1.c

Annex A – Security Target